EL AVANCE TECNOLÓGICO MUNDIAL Y LA SEGURIDAD INFORMÁTICA

Barranco, Jorge.
cabamajo@hotmail.com
Universidad Piloto de Colombia

Resumen - Vivimos en un mundo interconectado donde existe la posibilidad de ser víctima de un ciberdelincuente; y también tenemos la gran oportunidad de disfrutar más tiempo de calidad con los que más amamos, gracias a las TIC.

Summary. We live in an interconnected world where there is the possibility of being a victim of a cybercriminal; and we also have a great opportunity to enjoy more quality time with what we love through TIC.

Palabras claves. Análisis de riesgo, ataques informáticos, crisis global, ciberterrorismo, entorno inteligente.

I. INTRODUCCIÓN

El estado colombiano, el gobierno nacional, las distintas entidades encargadas de garantizar la seguridad y los derechos de los colombianos, han presentado con el desarrollo de la tecnología, nuevos desafíos para mantenerlos a salvo. Ha creado nuevas entidades, mejorado el reconocimiento de nuevos delitos, ha creado una legislación acorde con los estándares internacionales de cooperación para la prevención, y contrarrestar los ataques informáticos.

II. ATAQUES INFORMÁTICOS PROBLEMA DEL MUNDO

Desde los inicios de la humanidad siempre se ha buscado la paz y la seguridad, son los valores inherentes que todos buscamos, no sólo para nosotros, sino para todo cuanto nos rodea, es por ello que deseamos que toda nuestra información este protegida de personas mal intencionadas, que buscan causar un daño a nuestra intimidad o a nuestra economía.

Muchas personas dedican una parte importante de su vida a encontrar la seguridad que les permita enfrentar su día a día de forma diferente, apuntando siempre a la evolución; Pero encontrar la seguridad informática no es una tarea sencilla, requiere de cambios de hábitos y dedicación. Todos queremos sentirnos en paz, estar felices, vivir tranquilos, junto a los seres que amamos, pero ¿acaso estamos haciendo algo por conseguirlo? La seguridad informática, así como otras cualidades del bienestar, implica trabajo constante, por eso comienza, por plantear cuales son las herramientas de las que se dispone para alcanzar este objetivo. Detectar las cualidades que podrían dificultar el camino a la paz y la tranquilidad de vivir de un modo seguro, es un paso esencial. Por ejemplo, si es una persona nerviosa, mal humorada, ansiosa etc., estas emociones deberán ser controladas y neutralizadas para que pueda evolucionar y mantenerse alerta, donde quiera que se encuentre, ya que sin saberlo estamos dejando pistas sobre nuestro perfil, hábitos y costumbres. Esto es lo que buscan las personas mal intencionadas para cometer delitos, perjudicando y dañando nuestro bienestar y tranquilidad.

Alcanzar la protección de nuestros datos no debería resultar difícil. Debemos encontrar quien nos ayude a superar estos problemas, para mejorar nuestro bienestar. Algunas personas acuden a un técnico, otras a un amigo o algún conocido, otras simplemente prefieren hablar que el problema es del estado. Elija la alternativa que lo haga sentir más cómodo. Aprenda a darle a las cosas su justo valor. Muchas veces nos preocupamos o frustramos con pequeñeces que tienen solución, esto nos llena de tensión y nos impide sentirnos en paz.

El progreso de las tecnologías de la información y las comunicaciones, han estimulado un cambio de los prototipos, que exige adoptar nuevas herramientas especializadas y desarrollar procedimientos para neutralizar y controlar las amenazas cibernéticas. Es un nuevo interés creciente a nivel mundial, en el contexto de los estudios de ciencia, tecnología y sociedad. Reducir la incertidumbre y aumentar la eficiencia en la gestión, mejorando su capacidad de respuesta en entornos cambiantes en nuestro mundo digital, cada vez más globalizado.

En la valoración de la actividad, es la eficiencia productiva, es decir, será eficiente si se obtiene el máximo rendimiento de los factores productivos que utiliza, sin derrochar recursos, para nadie es un secreto que debemos invertir en nuestra seguridad informática,

debido a los crecientes ataques cibernéticos realizados por personas maliciosas, que atentan contra nuestra integridad, la información y la privacidad, es por ello que todo el dinero invertido en seguridad informática no está de más, así como hacen los ejércitos convencionales, así mismo nosotros debemos proteger nuestra información.

Manuel Castell nos dice: "Los ciudadanos que estén informados y que estén articulados en las nuevas tecnologías, pero al mismo tiempo mantengan su identidad, su cultura y su ciudadanía, son aquellos que serán más capaces de crear, producir conocimiento, e información, y en último término, valor en una economía que es la información y el conocimiento"[15]. La educación tiene que cambiar, dejar a un lado el mundo que fue y prepararnos para estos nuevos retos, en el nuevo mundo.

Ciberespacio, se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el mundo físico va más allá que el de escribir. La información se puede intercambiar en tiempo real o en tiempo diferido, y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar. Hace solo algunos años, las personas se comunicaban por cartas, las cuales duraban meses en recorrer nuestro país, o cuando se hacían negocios en cheques; por ejemplo, entre Barranquilla y Agustín Codazzi el cheque demoraba seis meses para saber si tenía o no fondos.

El mundo actual ha visto recientemente una nueva forma de ataques no bélicos, pero de gran importancia, en la que se ha visto comprometida su seguridad, debido a la divulgación de información clasificada, secretos militares, y cables diplomáticos, que han puesto en entredicho las relaciones internacionales entre distintos países. En el año de 2007 el gobierno de Estonia sufrió el mayor ataque informático de la historia donde se vieron afectados el gobierno nacional y grupos bancarios, lo que llevo a los organismos internacionales en el 2008 a reaccionar, para la protección de sus integrantes mediante la creación del Centro de excelencia para la Cooperación en Ciberdefensa (CCD), un comité de naturaleza europea pero con extensión mundial, de igual forma ha sido atacado el gobierno estadounidense, y sus distintas dependencias. El sector privado también ha sido blanco de estos asaltos lo que ha significado gastos de grandes firmas en su presupuesto de seguridad de más de dos millones de dólares anuales, siendo el más reciente el de SONY, con divulgación de sus nóminas, proyectos, y comunicación entre altos ejecutivos quienes se han visto abocados a presentar disculpas por sus conversaciones privadas. [2].

III. POLÍTICAS DE CIBERSEGURIDAD – DEFENSA EN COLOMBIA

La amenaza informática también ha generado que Colombia busque mecanismos para la prevención y control del delito. Ha debido actualizar su normatividad debido a que la tecnología presenta cambios constantes a la par de las amenazas informáticas. El gobierno nacional bajo su compromiso de garantizar la seguridad y defensa del estado de forma integral, ha implementado tres objetivos en cuanto a la ciberseguridad: 1) Implementar instancias apropiadas para prevenir, atender, controlar, y proteger la infraestructura. 2) Diseñar y ejecutar planes para la realización de capacitación a nivel especializado. 3) Buscar el fortalecimiento de la normatividad. [1].

La legislación colombiana ha venido evolucionando a través del tiempo en el tema de seguridad, en el ciberespacio en el año de 1999 mediante la ley 527, el estado reconoció el comercio electrónico, la creación de firmas digitales, y los mecanismos de certificación de estos [3]. En el 2000 el código penal crea la figura del bien jurídico de los derechos de autor y delitos informáticos [4]. En el 2009 se dan medidas para la protección informática y datos, en este mismo año se da la creación de la Agencia Nacional del Espectro encargada de Realizar la planeación, atribución, vigilancia y control del espectro [5]. Colombia ha firmado convenios internacionales como el del consejo europeo del 2004, buscando facilitar la prevención de las conductas delictivas y dar herramientas eficaces para detectar, investigar y sancionar a los infractores tanto en el territorio nacional como internacional. La creación de redes hemisféricas de cooperación como las creadas con la Organización de los Estados Americanos (OEA) y la comunidad andina.

El país en su autoevaluación acerca de la seguridad ha notado que presenta grandes debilidades, debido a que no se cuenta con una estrategia nacional apropiada y la no coordinación de entidades interinstitucionales, limitando su capacidad de reacción en operaciones de ciberseguridad y ciberdefensa, debido también al conocimiento limitado y la oferta académica del tema en el país.

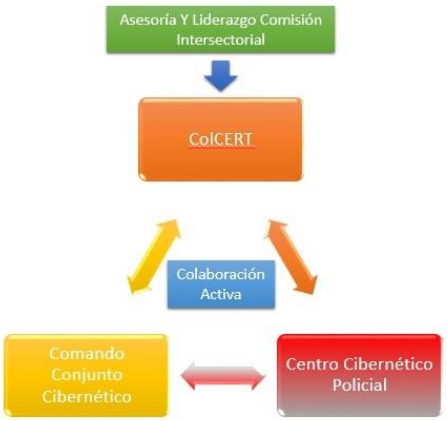

Fig. 1 Modificado de: Documento Conpes 3701. [1].

En esta medida se ha organizado el grupo de respuesta a Emergencia Cibernética de Colombia (ColCERT), quien se encuentra liderado por el Ministerio de Defensa Nacional, que tiene como primera función fortalecer al estado para enfrentar las amenazas contra su seguridad y defensa en el ámbito cibernético dando las herramientas necesarias, se encuentra conformado además por los Ministerios de Interior y del Derecho, Justicia, Relaciones Exteriores, de las Tecnologías de la Información y las Comunicaciones, la Policía Judicial, el Departamento Nacional de Planeación y la Fiscalía General de la Nación, a nivel de la colaboración intersectorial, a nivel operativo presenta una integración de el Comando Conjunto Cibernético (CCOC) en manos de las fuerzas militares y su mando general que protegen el país en el ciberespacio, defendiéndolo de software maliciosos, ejecución de protocolos de ciberdefensa, la protección de la infraestructura y desarrollo de capacidades de neutralización[1]. El Centro Cibernético Policial (CCP) se encuentra encargado de proteger la ciudadanía de amenazas y delitos cibernéticos, mediante la prevención, concienciación, investigación acerca de vulnerabilidades e incidentes que pongan en riesgo la infraestructura informática crítica de la nación [1].

IV. ORIGEN

Tiene su origen en la palabra griega cibernao (pilotear una nave), se empleó por primera vez en la novela de ciencia ficción, neuroamante escrita por Willian Ford Gibson en 1984, y a partir de ahí se popularizó su uso [16].

Fig. 2 Contacto Mundial – Internet. [3].

La vertiginosa evolución y acogimiento de las TIC como plataforma para cualquier diligencia socioeconómica, el creciente uso de las mismas por toda la sociedad, la fulminante expansión de las redes de telecomunicaciones, y el fenómeno de convergencia, han marcado la dinámica del sector de las TIC y las economías de los países durante los últimos años; y la seguirán marcando, ya que las tendencias internacionales muestran que el ambiente digital es dinámico y crece consecutivamente.

En el entorno se ha consolidado una economía basada en tecnologías, con el fin de abordar las incertidumbres, los riesgos, las amenazas, las debilidades y los incidentes digitales; en el 2011, el gobierno nacional expidió el documento CONPES 3701, un lineamiento de política para ciberseguridad y ciberdefensa, esta política concentró los esfuerzos del país en neutralizar el ensanchamiento de las amenazas informáticas que lo afectaban y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética.

La capacitación y adiestramiento se han fortalecido desde diferentes frentes, en aspectos como campañas de sensibilización para el uso responsable de Internet con énfasis en niños y jóvenes, hasta el suministro de formación especializada a servidores públicos.

V. ANÁLISIS DE RIESGO

El primer pasó en la administración del análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus flaquezas que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo[10].

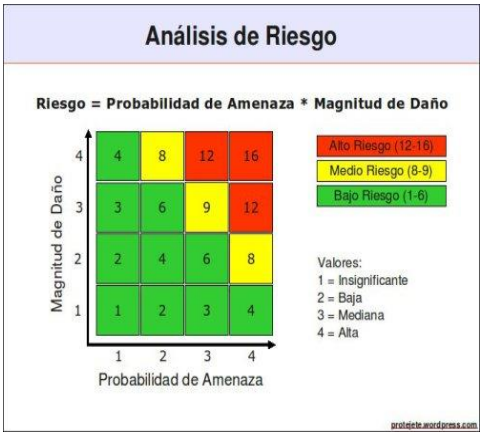

Fig. 3 Matriz de riesgos. [10].

VI. ¿QUÉ PUEDE DETONAR UNA CRISIS GLOBAL?

Los factores más importantes que pueden desatar una crisis global son aspectos a los que todos los habitantes del mundo estamos expuestos a diario:

- Economía.
- Amenazas de la naturaleza.
- Geopolítica.
- Aspectos Sociales.
- Tecnología.
- El impacto cibernético.
- Otra.

Es nuestra obligación preparar los métodos necesarios y tener un análisis de los riesgos en nuestros equipos de computación para disminuir los riesgos de ataques cibernéticos.

Para estimar la probabilidad de amenaza nos podemos hacer algunas preguntas:

A. ¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos?

Uno de los motivos para ser atacados, puede ser el manejo de información comprometedora, novedades, cifras, contabilidad, etc. La presencia de competencia directa en el trabajo, negocio, investigación, etc.; o por ser un personaje público.

B ¿Cuáles son nuestras flaquezas?

Es importante considerar todos los grupos de vulnerabilidades; también se recomienda incluir los expertos, especialistas de las diferentes áreas de trabajo para obtener una imagen más completa y más detallada sobre la situación interna y el entorno.

C. ¿Cuántas veces ya han tratado de atacarnos?

Ataques pasados nos sirven para identificar una amenaza, y si su ocurrencia es frecuente, más grande es la probabilidad que pasará otra vez. En el caso de que ya tengamos implementadas medidas de protección es importante llevar un registro, que muestre los casos, cuando la medida se aplicó exitosamente y cuando no; Porque así sabemos, en primer lugar si todavía existe la amenaza, y cuál es su riesgo actual.

El considerar todos los puntos anteriores, nos permite clasificar la probabilidad de amenaza. Sin embargo, antes tenemos que definir el significado de cada condición de la probabilidad (baja, mediana, alta). Las definiciones mostradas en la imagen anterior (Fig. 3), solo es un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propias condiciones.

D. ¿Cuándo hablamos de impacto?

Se pierde la información o conocimiento que tenemos acerca de nosotros o de la empresa donde laboramos lo que hace que sea atractivo al delincuente.

- Terceros tienen acceso a la información.
- La información ha sido manipulada.
- Desconfianza de la información ya que no sabemos si se suprimieron algunos apartes o si modificaron la fuente.

Estimar la magnitud de daño generalmente es una tarea muy compleja; La manera más fácil, es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considere otros valores como daños materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso. Porque nos sentimos desnudos cuando no sabemos aún a ciencia cierta que ha ocurrido en nuestro ambiente y no sabemos cómo resolver la situación entramos en un descontrol total.

Aunque conozcamos bien el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde manejamos la información, sea en una ONG (derechos humanos, centro de información etc.), en una empresa privada (banco, clínica, producción etc.), en una institución estatal o en el ámbito privado. Otro factor

decisivo, respecto a las consecuencias, es también el entorno donde nos ubicamos, es decir cuáles son las leyes y prácticas comunes, culturales que se aplica para sancionar el incumplimiento de las normas.

Un punto muy esencial en el análisis de las consecuencias, es la diferenciación entre los dos propósitos de protección de la seguridad informática, la seguridad de la información y la protección de datos, porque nos permite determinar, quien va a sufrir el daño de un impacto, nosotros, nuestros comportamientos y decisiones deben ser dirigidos por una conciencia responsable, de no causar daño a otros, aunque su realidad no tenga consecuencias negativas. Muchas veces lo que comienza como un juego termina afectando a muchos, sin tener la mínima intención de actuar malignamente.

VII. CIBERTERRORISMO

Con el surgimiento de las tecnologías de información también se abrió una compuerta para la comisión de delitos a través de las mismas. Históricamente las leyes penales surgen como una respuesta a las actividades que producen daño a la sociedad y con la aparición de los computadores, comenzaron nuevos delitos y la preocupación por castigar ciertas conductas, recibiendo el nombre de delitos informáticos. Podemos establecer que el ciberterrorismo, es la forma de terrorismo que utiliza las tecnologías de información para acobardar, coercionar o para causar daños a grupos sociales con fines políticos-religiosos [13].

El desarrollo de la informática y la incorporación de la misma a nuestra vida cotidiana, confirma su presencia en la mayoría de los países incluyendo hasta los del tercer mundo a nivel gubernamental. Las telecomunicaciones se están moviendo velozmente hacia la Internet como canal preferencial. La mundialización ha encontrado un mecanismo de facilitación en la internet de banda ancha y el comercio; las nuevas formas de hacer negocios se orienta hacia la conexión directa con los consumidores gracias a ella. En la administración de empresas es una meta llegar a la oficina sin papeles y el trabajo telemático desde casa se hace una clara opción para la reducción de costos operacionales. Esto ha ayudado al medio ambiente por la reducción en el uso de papeles y el trabajo más eficiente, puesto que muchas personas ya no tienen la necesidad de salir de sus hogares hasta la oficina a laborar y esto ha hecho que el tiempo muerto en el tráfico lo maximice en su trabajo.

Las tecnologías de información están ganando cada día preponderancia en las operaciones de control de sistemas administrativos, de seguridad y vigilancia. La tecnología militar en la actualidad depende en gran parte de la informática, así como los mecanismos de preservación y análisis de información de red, nació de la idea y de la necesidad de establecer múltiples canales de telecomunicación entre computadores. En caso de un ataque nuclear que eliminará líneas de conexión existentes, se utilizarían medios alternos de conexión informática sin importar la ruptura de otras líneas o canales de conexión.

Entonces la idea de este tipo de redes fue la de garantizar las telecomunicaciones militares con fines de seguridad y defensa en los Estados Unidos en Norteamérica. Esta red conocida como Arpanet fue desarrollándose de tal forma que evolucionó paralelamente con la red pública para uso de universidades bajo este mismo concepto múltiples conexiones telemáticas.

Los grupos extremistas requieren de fondos para mantenerse; se ha comprobado que diversos grupos terroristas incurren en otros tipos de delitos como la piratería para obtener dinero; la red, es un medio ampliamente utilizado para la transferencia ilegal de software y de películas.

Ciberterroristas están realizando extorsión a grupos financieros para recaudar fondos a cambio de no ser ciberatacadas, por lo que aquellos que realizan estos pagos bajo amenazas, para no ser atacadas informáticamente o bien para no revelar datos de clientes, contra delitos informáticos que podemos llamar "*cibervacunas*".

El anonimato es una de las ventajas de las telecomunicaciones informáticas. Son conocidos varios casos en los que secuestradores y extorsionistas utilizan el correo electrónico y el chat para pedir rescate o sumas de dinero.

La planificación de ataques y la comunicación entre miembros de células terroristas puede establecerse desde cualquier cibercafé de forma asíncrona vía correo electrónico, en vivo o vía chat.

En la medida que la digitalización y adopción de nuevas tecnologías sea cada vez mayor, nuestra calidad de vida mejorará. El potencial de las TIC para generar prosperidad será imparable.

En un estudio revela que en 20 años, el impacto positivo a nivel global, una reducción del 20% en las emisiones de carbono, más de 11 billones de dólares en nuevos beneficios económicos, atención sanitaria online para 1,600 millones de personas y un aumento del 30% en

los rendimientos agrícolas. Todo ello, gracias a la adopción de nuevas tecnologías que son cada vez más rápidas, económicas y accesibles.

La oportunidad de 11 billones de dólares demuestra que las TIC pueden mejorar los negocios, al invertir en productos y servicios que son social y ambientalmente responsables. Las nuevas tecnologías ya no son sólo más accesibles, sino capaces de generar un impacto directo para mejorar la calidad de vida de las personas, inclusive en una escala masiva al habilitar modelos de negocio que se vuelven una fuente de competencia y crecimiento sostenido.

Existen tres factores que aceleran el potencial de las TIC para generar prosperidad:

- Las tecnologías actuales ponen al usuario como el centro de las soluciones. Los individuos cada vez están más empoderados y pueden acceder a más servicios de salud, aprendizaje y consumo.
- Las TIC están habilitando modelos de negocios que buscan depender cada vez menos del carbono y del uso de recursos naturales.
- Desde la iniciativa privada debemos reconocer las oportunidades de crecimiento e innovación que ofrecen las nuevas tecnologías y que harán viables las inversiones sustentables.

Es necesario establecer metas corporativas para reducir el nivel de emisiones de carbono y de desperdicios generados, así como promover iniciativas ecológicas entre los empleados.

Es importante que los ciudadanos adopten soluciones tecnológicas que promuevan el uso eficiente de los recursos. Aprovechar las herramientas de capacitación y nuevos servicios que vienen con la digitalización, y promover su uso consciente y responsable, también será una prioridad.

A medida que estas iniciativas avancen y la digitalización y adopción de nuevas tecnologías sea cada vez mayor, nuestra calidad de vida mejorará.

El potencial de las tecnologías de la información para generar prosperidad será imparable.

El más reciente informe del DANE, indica que el sector de telecomunicaciones y correos creció en septiembre de 2011, a 9,5% frente al mismo mes del año anterior, 1,8 puntos más que el resto de la economía, que creció 7,7%. Este crecimiento de la industria TIC, es el mayor en los últimos 14 trimestres, es decir el resultado más positivo de los últimos cuatro años en Colombia. Comparando las grandes ramas de la economía, los sectores de transportes y comunicaciones fueron los terceros con mayor crecimiento entre septiembre de 2010 y septiembre de 2011, sólo superados por los sectores de la construcción y la explotación minera. [17] Es una excelente noticia para todos los colombianos dada la enorme importancia que tiene las TIC en el desarrollo del país. La internet es una herramienta clave para jalonar prosperidad y disminuir la pobreza en Colombia. El resultado se sustenta en muy importantes logros, en particular el impulso dado por la banda ancha al sector TIC. En el 2007, cuando el sector crecía a dos dígitos, la penetración celular era de tan sólo 67% y el crecimiento del sector TIC se explicaba por el aumento de la telefonía móvil. Actualmente, la penetración móvil es superior a 103% y el crecimiento de la industria TIC se explica por el incremento de banda ancha con el programa vive digital, ha permitido que Colombia dé un salto de 2,2 millones de conexiones a 4,6 en la actualidad. En el 2011 logramos 1.5 millones de nuevas conexiones de internet de banda ancha para un crecimiento de 49,5 de esa conectividad. Llevamos subsidios para Internet a 115 mil hogares de estratos 1 y 2. Tenemos 325 municipios conectados actualmente a la red nacional de fibra óptica.

En los últimos años, han surgido múltiples amenazas en contra de la infraestructura interconectada. Esta es altamente vulnerable y si se atenta contra ella, puede llegar a paralizarse completamente un país. Las amenazas cibernéticas tienen una connotación sustancialmente diferente a la de otras amenazas a la seguridad nacional; dado que éstas pueden tener diferentes objetivos pueden ser realizadas por diferentes tipos de actores (crimen organizado, terroristas o estados), su costo es mínimo y su trazabilidad es sumamente difícil.

En los últimos años, se han detectado múltiples intentos de ataque a la infraestructura crítica del país. Estos intentos han sido neutralizados exitosamente hasta el día de hoy, sin embargo, su nivel de sofisticación cada vez es mayor y por lo tanto, se requiere un equipamiento de última tecnología y una excelente preparación del personal a cargo de la seguridad nacional de Colombia.

Al beneficiarnos de los ilimitados recursos de las redes públicas, de datos como internet y de la infraestructura tecnológica interconectada, también nos enfrentamos a nuevos escenarios para el delito, el terrorismo y la guerra, lo cual exige la creación de nuevas herramientas de prevención, reacción y defensa. Para consolidar una capacidad suficiente de ciberseguridad y ciberdefensa.

Los riesgos de un ataque cibernético a las redes interconectadas del país son cada vez más altos, cuanto más se extienda el uso de internet en nuestro país y se aumente la dependencia a las infraestructuras y tecnologías informáticas, el nivel de vulnerabilidad se incrementará.

La seguridad informática en Colombia y el mundo es un nuevo reto que se le ha impuesto a la humanidad dado el avance tecnológico que indudablemente ha traído beneficios, pero ha desencadenado igualmente nuevos delitos, lo que ha llevado a buscar a los distintos gobiernos, a los organismos internacionales y el sector privado a buscar maneras de proteger su información, la de sus ciudadanos y la de sus usuarios; mediante la legislación, la educación, la promoción de la seguridad, y medidas para blindarse de ataques cibernéticos contra las actividades que se realizan en el ciberespacio.

VIII. UN ENTORNO INTELIGENTE

(Smart environment). Se refiere al uso de las nuevas tecnologías para proteger y preservar el entorno de la ciudad [14].

Hablamos de factores como la seguridad y confianza, mediante la implementación mediante el uso de las TIC algún sistema para mejorar la seguridad ciudadana y el de la promoción y preservación de la identidad cultura, mediante el impulso de alguna de iniciativa para digitalizar y compartir su patrimonio cultural.

Los principales resultados de los diferentes estudios:

- Cada vez es mayor el número de ciudades que han implementado mediante el uso de las TIC algún sistema para mejorar la seguridad ciudadana en su territorio.
- El principal sistema utilizado es vídeo vigilancia.
- También se utilizan las nuevas tecnologías en la mejora de los sistemas informáticos, para gestionar incidencias y emergencias.
- Cada vez es mayor el número de ciudades que han impulsado alguna iniciativa para digitalizar y compartir su patrimonio cultural, en especial en las ciudades de Asia y Europa.

Fig. 4 Nuestro mundo. [14].

Todos los pasos para vivir en un ambiente sano y seguro dependerán del grano de arena que cada uno ponga, ya que la seguridad comienza en casa, enseñando a nuestros hijos la manera responsable de utilizar los recursos disponibles, como son la tablet, computador, teléfono inteligente, todo ello con una buena conciencia. Como dice un proverbio alemán: “La mejor almohada, es una conciencia tranquila”.

La seguridad es un factor imprescindible en todos los espacios profesionales y en la informática, es especialmente significativo porque en los ordenadores es donde está almacenada la información privada de una empresa o de cualquier persona. En la actualidad la información es un objeto de valor para las compañías. Por esto y otros motivos, la seguridad de la información es un asunto tan trascendente para todos, pues afecta directamente a las actividades comerciales de una empresa o de un particular. La seguridad informática es una forma de comunicarse con los usuarios, con ella se establece un canal donde fluye toda la comunicación, los recursos y los servicios, de las organizaciones modernas.

No es una camisa de fuerza de protocolos técnicos o claves de seguridad en ella están inmersas las conductas de los empleados y las políticas de la empresa, ya que en ella está implícito todo lo que deseamos resguardar; cada empleado debe estar atento y alerta, por el uso y conocimiento de la información que maneja de los servicios informáticos. La seguridad es un conjunto de requisitos definidos por los responsables de un sistema, son ellos que nos indican la manera correcta, que se puede y que no por los protocolos de seguridad durante la operación general. La seguridad cubre los sistemas informáticos y proporcionan la base para definir responsabilidades en la actuación de cada uno.

A partir de sus bases, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con un arsenal informativo documentado y

normalizado, dedicado a la estandarización del método de operación de cada uno de los individuos involucrados en la gestión de la seguridad.

IX. RECOMENDACIONES

Según los entes que integran todos los organismos que trabajan con la seguridad en la información, los organismos del gobierno y el documento del Consejo Nacional de Políticas Económicas y Social (CONPES) dependencia del departamento de planeación nacional, recomienda [7]: 1) Implementar la institucionalidad apropiada [1]. Que busca maximizar la seguridad en la red de los distintos estamentos del estado, el sector privado y la ciudadanía en general. 2) Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa, mediante la cual se dan bases para propiciar el estudio e investigación, para detectar las vulnerabilidades que se presentan y que serían las amenazas por medio de las cuales pueden resultar afectado el estado o cualquier habitante del país. 3) Fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa. [1] Dando pie a la integración internacional para prevenir los ciberataques y realizar conjuntamente investigación y fortalecimiento para responder oportunamente a los ataques que a diario se vive en la red.

X. CONCLUSIONES

De la revisión acerca de cómo Colombia se encuentra en materia de ciberseguridad y ciberdefensa, podemos afirmar que el país se encuentra realizando esfuerzos notorios, mediante la legislación, el intento de organizar un eje de respuesta de los entes de seguridad del estado que funcione como engranaje para defenderse de los ataques al que se encuentran sometidos los usuarios de internet, tanto en la estructura física, como en los programas informáticos que se usan, debido a la preocupación constante acerca de que sea atacada la confidencialidad, integridad y disponibilidad de la información, no tan solo de los usuarios, sino también de las empresas del sector público y privado. Aún falta mucho camino por recorrer debido a la dinámica constante propia de la naturaleza informática que exige una mayor formación académica como plataforma fundamental para la preparación y respuesta a los distintos retos que se presentan a diario.

REFERENCIAS

[1] Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación, LINEAMIENTOS Conpes 3701 de 2011 – Lineamientos Ciberseguridad y Ciberdefensa.

[2] El tiempo-Asalto de Sony, http://www.eltiempo.com/tecnosfera/novedades-Tecnología/asalto-cibernético-que-desnudo-a-Sony/14941462.

[3] Ley de comercio electrónico en Colombia “Ley 527 de 1999”, http://www.alfa-redi.org/node/9828.

[4] Código Penal-“Ley 1273 de 2009”, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

[5] Agencia Nacional del Espectro-Misión y Visión http://www.ane.gov.co/index.php/conozca-la-Ane/misión-y-visión.html.

[6] Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación, LINEAMIENTOS Conpes 3854 de 2016 – Política Nacional de Seguridad Digital.

[7] http://www.laopinion.com.co/tecnologia/empresas-invierten-poco-en-seguridad-informatica.

[8] https://elcibeterrorismo.wordpress.com/2015/06/.

[9]https://protejete.files.wordpress.com/2009/07/gestion-de-riesgo-en-la-seguridad-informatica.pdf.

[10]https://protejete.wordpress.com/gdr_principal/analisis_riesgo/.

[11]http://manuelcarballal.blogspot.com.co/2010/04/ciber crimen-y-ciberdelito.html.

[12] http://altec-ltda.cl/bio.htm.

[13] http://barriosyvecinos.com.co/latinoamerica-esta-lista-para-vivir-un-entorno-digital-inteligente/

[14] http://www.redalyc.org/articulo.oa?id=86020052039.

[15] http://www.ecured.

[16] http://www.mintic.gov.co/portal/604/w3-article-2668.html.

Jorge Mario Barranco Carvajal, Ingeniero de Sistemas de la Universidad Popular del Cesar.

Estudiante de la "Especialización en Seguridad Informática" de la Universidad Piloto de Colombia de 2016.